Confirmation No. 4003

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	PESSOLANO	Examiner:	King, John B.
Serial No.:	10/553,790	Group Art Unit:	2435
Filed:	October 19, 2005	Docket No.:	NL030397US1 (NXPS.589PA)
Title:	ELECTRONIC CIRCUIT DEVICE FOR CRYPTOGRAPHIC APPLICATIONS		

APPEAL BRIEF

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Customer No.
65913

Dear Sir:

This Appeal Brief is submitted pursuant to 37 C.F.R. §41.37, in support of the Notice of Appeal filed July 28, 2011, and in response to the rejections of claims 1-8 and 13-14, as set forth in the Final Office Action dated April 28, 2011.

Authorization is provided to charge Deposit Account 50-4019 (NL030397US1) **$620.00** for filing this brief in support of an appeal as set forth in 37 C.F.R. §1.17(c). If necessary, authority is given to charge/credit any additional fees/overages related to this filing.

I. Real Party In Interest

The real party in interest is NXP Semiconductors. The application is presently assigned of record, at reel/frame nos. 017887/0017 to NXP, B.V., headquartered in Eindhoven, the Netherlands.

II. Related Appeals and Interferences

While Appellant is aware of other pending applications owned by the above-identified Assignee, Appellant is unaware of any related appeals, interferences or judicial proceedings that would have a bearing on the Board's decision in the instant appeal.

III. Status of Claims

Claims 1-8 and 13-14 stand rejected and are presented for appeal. A complete listing of the claims under appeal is provided in an Appendix to this Brief.

IV. Status of Amendments

An amendment was filed on June 28, 2011 in response to the Final Office Action dated April 28, 2011. The Advisory Action dated July 18, 2011 indicates that the amendment was entered. No further amendments have been filed.

V. Summary of Claimed Subject Matter

As required by 37 C.F.R. § 41.37(c)(1)(v), a concise explanation of the subject matter defined in the independent claims involved in the appeal is provided herein. Appellant notes that representative subject matter is identified for these claims; however, the abundance of supporting subject matter in the application prohibits identifying all textual and diagrammatic references to each claimed recitation. Appellant thus submits that other application subject matter, which supports the claims but is not specifically identified above, may be found elsewhere in the application. Appellant further notes that this summary does not provide an exhaustive or exclusive view of the present subject matter, and Appellant refers to the appended claims and their legal equivalents for a complete statement of the invention.

Commensurate with independent claim 1, an example embodiment of the present invention is directed to an electronic circuit device for executing operations dependent on secret information. *See, e.g.*, Fig. 1. The electronic circuit device includes power supply connections, a processing unit, an activity monitor circuit and a current drawing circuit. *See, e.g.*, Fig. 1 and discussion of 10, 12, 14, 16 and 18 at page 4:1-13. The processing unit includes a plurality of processing circuits for use in execution of respective parts of the operations dependent on the secret information, the processing circuits being fed from the power supply connections. *Id.* The activity monitor circuit is coupled to receive pairs of processing signals, each of the pairs of processing signals including an input signal and an output signal of one of the processing circuits. *See id.* and page 4:14-29. The activity monitor circuit receives a pair of processing signals for each of the processing circuits, coming into and out of the processing circuit respectively, and derives activity information from each pair of processing signals, with the activity information being indicative of whether each of the processing circuits generates a logic level transition. *Id.* The activity monitor circuit also derives, from the activity information, a combined activity signal indicative of a sum of power supply currents that will be consumed by the processing circuits dependent on the processing signals indicative of the sum of power supply currents that will be consumed by said processing circuits in combination. *Id.* The current drawing circuit is connected to the power supply connections and controlled by the activity monitor circuit to draw a cloaking current controlled by the combined activity signal, so that power supply current variations dependent on the secret information are cloaked in a combination of the cloaking current and current drawn by the processing circuits. *See id.* and page 5:26-34 and 7:1-5, with Figure 2. The activity monitor circuit is coupled to the current drawing circuit to control generation of the cloaking current under control of the combined activity signal. *See id.* and page 2:24-29.

Commensurate with independent claim 7, another example embodiment of the present invention is directed to a method of executing operations dependent on secret information in an electronic circuit. *See, e.g.*, Fig. 1 and discussion of 10, 12, 14, 16 and 18 at page 4:1-13. Power supply current is supplied to processing circuits, and respective parts of operations that depend on the secret information are executed using the processing circuits. *Id.* Pairs of processing signals coming into and out of each of the

processing circuits are received, each of the pairs of processing signals including an input signal and an output signal of one of the processing circuits. *See id.* and page 4:14-29. Activity information is derived from each pair of processing signals, the activity information indicative of whether each of the processing circuits generates a logic level transition. *Id.* A combined activity signal is derived from the activity information, and is indicative of a sum of power supply currents that will be consumed by all of the processing circuits in combination dependent on the processing signals. *Id.* A cloaking current controlled by the activity information is drawn, using the combined activity signal to control the generation of the cloaking current, and the cloaking current is combined with current drawn by the processing circuits so that power supply current variations dependent on the secret information are cloaked in the combination of the cloaking current and current drawn by the processing circuits. *See id.* and page 5:26-34 and 7:1-5, with Figure 2.

VI. Grounds of Rejection to be Reviewed Upon Appeal

The grounds of rejection to be reviewed on appeal are as follows:

A. Claims 1, 5, 7 and 13 stand rejected under 35 U.S.C. § 103(a) over Thüringer *et al.* (U.S. Patent No. 6,498,404)

B. Claims 2-4 stand rejected under 35 U.S.C. § 103(a) over Thüringer *et al.* (U.S. Patent No. 6,498,404) in view of Patterson *et al.* ("Computer Architecture: A Quantitative Approach") pp. 134-135, 1995

C. Claims 6, 8 and 14 stand rejected under 35 U.S.C. § 103(a) over Thüringer *et al.* (U.S. Patent No. 6,498,404) in view of Kitamura *et al.* (U.S. Patent No. 4,212,056)

VII. Argument

Appellant submits that the rejections rely upon a misinterpretation of the claims, and have not addressed aspects of the independent claims that limit the input and output signals to signals "coming into and out of the processing circuit." Appellant has presented this issue in Section 1 below, but this misinterpretation provides one of the main reasons for reversing all rejections.

1. All § 103(a) Rejections Rely Upon A Misreading Of The Claims, And Fail To Establish Correspondence To The Claimed Invention.

Appellant submits that all of the § 103(a) rejections, each of which relies upon the primary '404 reference, are based upon a misreading of the claims that overlooks various claim limitations and fails to establish correspondence. Using claim 1 as an example, the final Office Action failed to establish correspondence to the claimed invention including aspects directed to an activity monitor circuit coupled to receive and process pairs of input and output signals for each of a plurality of processing circuits, with each pair of signals "coming into and out of the processing circuit respectively." As such, the rejections fail.

More specifically, the rejections have not addressed aspects of the claims limiting the above-referenced input signal to a signal coming into a processing circuit. Instead, the Examiner appears rely upon an assertion that the claims "merely recite that the activity monitor receives a pair of signals (2 signals) for each processing circuit where one of the signals is an output signal from the processing circuit ... [and the] other signal in each pair of signals is not specifically defined in the claims." Appellant submits that this assertion that the input signal "is not specifically defined in the claims" is erroneous. As consistent with the above, claim 1 recites that "the activity monitor circuit is coupled to receive **a pair of processing signals** for each of the processing circuits, **coming into and out of the processing circuit respectively**" (emphasis added). Accordingly, the "input signal" is defined as a signal "coming into ... the processing circuit." The Examiner's reliance upon an assertion that the input signal "is not specifically defined in the claims" is thus clearly in error, and the final Office Action's failure to establish correspondence to these limitations renders the rejections improper.

In addition to the above, the final Office Action has provided no explanation as to how the cited "power connection" and the "power consumption of data processing device" would correspond to aspects of the claimed invention directed to input and output signals of a processing circuit, or as to how any power connection would correspond to a "signal" as claimed (*e.g.*, a logic signal carrying information). In addition, the final Office Action's assertion (at page 9) that the '404 reference "has multiple circuits" fails to establish that these multiple circuits of the '404 reference would be connected for actually receiving pairs of signals from a plurality of processing circuits as claimed. Moreover, the assertion that a "power connection" is the same as an "input signal" (*i.e.*, a logic signal as discussed above) is also erroneous, and fails to establish correspondence.

In view of the above, the final Office Action relies upon a misinterpretation of the claims in rejecting independent claim 1, and has failed to establish correspondence to multiple claim limitations. As the Office Action also relies upon the same misinterpretation in rejecting independent claim 7, the rejections of both independent claims 1 and 7, and thus of all claims that depend therefrom, are improper. Appellant believes that its traversals regarding this matter now stand uncontested in the record, and requests that all rejections be reversed.

2. All § 103(a) Rejections Rely Upon An Interpretation Of The Claims That Contradicts The Specification, In Contrast To Controlling Law.

Appellant submits that the § 103(a) rejections are also improper because they are based upon a reading of the claims that directly contradicts Appellant's specification. As discussed in Section 1 above, the final Office Action has overlooked aspects of the claimed invention that specifically define the respective signals, and in particular, has erroneously asserted that an "input signal" is not defined. The final Office Action then goes on to interpret the input signal as being a "power connection" in accordance with the '404 reference. However, this interpretation contradicts Appellant's specification, which stands in contrast with the requirements of the M.P.E.P. and relevant law. For example, in *Ex parte TECHNOFIRST S.A.*, the Board of Patent Appeals and Interferences stated

> "[W]hile giving claim terms their broadest reasonable interpretation is correct and proper, such interpretations need to be made in view of the specification. See Phillips v. AWH Corp., 415 F.3d 1303, 1316 (Fed. Cir. 2005). With such a standard, we do not find the Examiner's alternate interpretations to be consistent with the instant Specification."

Accordingly, the rejection cannot rely upon a proposed interpretation of a claim term that contradicts Appellant's specification.

As applicable here, referring to the example embodiments described in connection with processing circuit 102 in Figure 1 of Appellant's specification, pairs of input and output signals 110 and 112 are processed by an activity detection circuit 112a. Accordingly, the final Office Action's interpretation of the "first signal" as being any undefined signal such as a "power connection" would not only appear to involve a misreading of the claims, it would also involve an interpretation of the claims that is inconsistent with the specification, including those aspects as described in connection with Figure 1 above. This interpretation would also appear to contradict other example embodiments describing such activity detection circuits and processing circuits and/or related methods. For instance, example embodiments as described in connection with Figure 3 show that the input signal at 310 is a logic signal (*see, e.g.*, page 8:5-13). Interpreting the input signal as the power connection in the '404 reference would eviscerate this aspect of Appellant's disclosure. Appellant therefore submits that the proposed interpretation stands in contrast with the specification as cited above and otherwise.

Accordingly, all § 103(a) rejections are also improper for relying upon an interpretation of the claims that is inconsistent with the specification. Appellant therefore submits that the rejections of all claims should be reversed for these reasons as well.

3. The § 103(a) Rejections Lack Motivation As The Resulting Combination Of References Would Be Inoperable As Asserted.

Appellant further traverses the § 103(a) rejections over the '404 reference because the proposed modification of the '404 reference, to use a power connection as an input signal in accordance with the claimed invention, would result in a hypothetical embodiment that would be inoperable as claimed. When an asserted combination would render the invention inoperable, the obviousness rejection is invalid for lack of

motivation. *See In re Gordon*, 733 F.2d 900 (Fed. Cir. 1984). This is consistent with the recent *KSR* decision, the USPTO Guidelines under *KSR* and M.P.E.P. § 2143.01, which explains the long-standing principle that a § 103 rejection cannot be maintained when the resulting combination involves an inoperable embodiment. *See KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 417 (2007).

Appellant submits that the proposed hypothetical embodiments involving the '404 reference alone and/or in combination with either the Patterson or '056 reference are improper because the use of a "power connection" in place of an input signal (*i.e.*, carrying data) would not appear to be operable in accordance with the claimed invention. For example, it is unclear as to how a power connection could be used by an activity monitor to derive activity information (as relative to doing so from a pair of processing signals), such as in claim 1. As the final Office Action is silent as to any explanation for this matter, the record as it stands cannot support the rejections.

Moreover, as the '404 reference integrates its load circuit and data processing device for security reasons, the proposed modification's separation/interchanging of the circuits would undermine this purpose and render the resulting embodiment vulnerable to attacks as discussed in the '404 reference as those to be avoided (*see, e.g.*, columns 1:66-67 and 2:1-4). The final Office Action's attempt to rebut this teaching away relies upon an opinion regarding supposed benefits of interchangeability, and fails to address the teachings in the '404 reference as noted by the Appellant as teaching away. In particular, the reliance upon M.P.E.P. § 2144.04 in asserting that "making integral things separable is 'merely a matter of obvious engineering choice'" is misapplied, as such an "engineering choice" cannot stand in contrast to teaching away in the reference itself, consistent with the above-cited *KSR* decision and M.P.E.P. § 2143.01. Appellant further notes that the Advisory Action asserts that the '404 reference "actually teaches that the loading circuit and the data processing device can be separate" but fails to provide any citation supporting the assertion, and would further appear to constitute new grounds if introduced in an Examiner's Answer. The '404 reference's clear teaching away ("because the separation of the load circuit form the data processing data for the purpose of attempted discovery requires far more technical means …") stands uncontested in the record.

In view of the above, the proposed hypothetical embodiment would appear to be inoperable to function as claimed, and any modification of the primary '404 reference to include the derivation of activity information as above would thus also appear to be inoperable as asserted. Accordingly, under the *KSR* and *In re Gordon* decisions, as also consistent with M.P.E.P. § 2143.01, the rejections should be reversed.

VIII. Conclusion

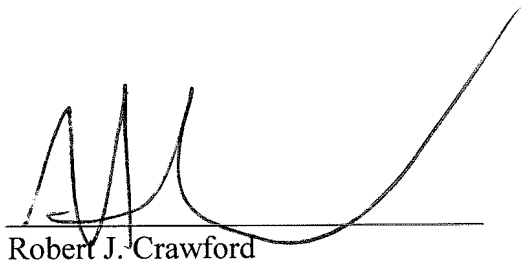
In view of the above, Appellant submits that the rejections of claims 1-8 and 13-14 are improper and therefore requests reversal of the rejections as applied to the appealed claims and allowance of the entire application.

Authority to charge the undersigned's deposit account was provided on the first page of this brief.

Please direct all correspondence to:

Intellectual Property & Licensing
NXP Semiconductors
411 East Plumeria Drive
San Jose, CA 95134

CUSTOMER NO. 65913

By: 

Robert J. Crawford
Reg. No.: 32,122
Eric J. Curtin
Reg. No. 47,500
651-686-6633
(NXPS.589PA)

APPENDIX OF CLAIMS INVOLVED IN THE APPEAL (S/N 10/553,790)

1. An electronic circuit device for executing operations dependent on secret information, the electronic circuit device, comprising:

power supply connections;

a processing unit comprising a plurality of processing circuits for use in execution of respective parts of the operations dependent on the secret information, the processing circuits being fed from the power supply connections;

an activity monitor circuit, coupled to receive pairs of processing signals, each of the pairs of processing signals including an input signal and an output signal of one of the processing circuits, the activity monitor circuit being arranged to derive activity information from each pair of processing signals, the activity information indicative of whether each of the processing circuits generates a logic level transition, and to derive from the activity information a combined activity signal indicative of a sum of power supply currents that will be consumed by the processing circuits dependent on the processing signals;

a current drawing circuit connected to the power supply connections and controlled by the activity monitor circuit to draw a cloaking current controlled by the combined activity signal, so that power supply current variations dependent on the secret information are cloaked in a combination of the cloaking current and current drawn by the processing circuits;

characterized in that the activity monitor circuit is coupled to receive a pair of processing signals for each of the processing circuits, coming into and out of the processing circuit respectively, the activity monitor circuit being configured to derive the activity information from each pair of processing signals and to derive from the activity information for said processing circuits the combined activity signal dependent on the processing signals indicative of the sum of power supply currents that will be consumed by said processing circuits in combination; the activity monitor circuit being coupled to the current drawing circuit to control generation of the cloaking current under control of the combined activity signal.

2. An electronic circuit device according to Claim 1, wherein the processing unit comprises a clock circuit, combinatorial logic circuits and registers clocked by the clock circuit and connected between respective parts of the combinatorial logic circuits, the pairs of processing signals comprising pairs of input and output signals of the registers, the current drawing circuit being arranged to adjust a value of the cloaking current dependent on the activity of the registers at instants synchronized by the clock circuit.

3. An electronic circuit device according to Claim 2, organized as a pipe-line of successive parts of the combinatorial logic circuits, each pair of successive parts coupled via a respective one or respective ones of the registers, the electronic circuit device, comprising:

a plurality of activity monitor circuits each coupled to receive pairs of input and output signals of the respective one or ones of the registers between a respective pair of successive parts of the combinatorial logic circuits, and to derive a combined activity signal from the pairs of input output signals;

a plurality of current drawing circuits connected to the power supply connections, each controlled by a respective one of the activity monitor circuits to draw a cloaking current controlled by the combined activity signal derived by that respective one of the activity monitor circuits.

4. An electronic circuit device according to Claim 3, arranged to activate the current drawing circuits in selected clock cycles, when the corresponding pipe-line stages process secret information.

5. An electronic circuit device according to Claim 1, having a trigger input coupled to the current drawing circuit, arranged to enable drawing of the cloaking current only upon receiving a trigger signal that triggers or accompanies execution of a secret information dependent process in the electronic circuit device.

6. An electronic circuit device according to Claim 1, comprising a reference current pattern generator, the current drawing circuit being arranged to adjust the value of the

cloaking current so that the combination of the cloaking current and current drawn by the processing circuits substantially equals a temporal reference current pattern generated by the reference current pattern generator.

7. A method of executing operations dependent on secret information in an electronic circuit, the method comprising:

supplying power supply current to processing circuits;

executing respective parts of operations that depend on the secret information using the processing circuits;

receiving pairs of processing signals coming into and out of each of the processing circuits, each of the pairs of processing signals including an input signal and an output signal of one of the processing circuits;

deriving activity information from each pair of processing signals, the activity information indicative of whether each of the processing circuits generates a logic level transition;

drawing a cloaking current controlled by the activity information, and combining the cloaking current with current drawn by the processing circuits so that power supply current variations dependent on the secret information are cloaked in the combination of the cloaking current and current drawn by the processing circuits,

characterized by

deriving from the activity information a combined activity signal indicative of a sum of power supply currents that will be consumed by all of the processing circuits in combination dependent on the processing signals; and

controlling generation of the cloaking current with the combined activity signal.

8. The method of claim 7, further comprising determining the cloaking current by subtracting the sum of power supply currents from a temporal reference current pattern.

13. The electronic circuit device of claim 1, wherein the current drawing circuit is a digital to analog converter that is configured to convert a digitally coded value into an analog power supply current that is equal to the cloaking current.

14. The electronic circuit device of claim 6, further comprising a subtractor that is configured to determine the cloaking current by subtracting the sum of power supply currents from the temporal reference current pattern generated by the reference current pattern generator.

APPENDIX OF EVIDENCE

Appellant is unaware of any evidence submitted in this application pursuant to 37 C.F.R. §§ 1.130, 1.131, and 1.132.

APPENDIX OF RELATED PROCEEDINGS

As stated in Section II above, Appellant is unaware of any related appeals, interferences or judicial proceedings.